Outcomes Star™ Online Information Governance Statement

Date of last update 4th April 2024

Contents

1. Introduction

This Information Governance Statement is the overarching policy for data security and protection for the Star Online web application (hereby known as “the Star Online” or “the application”.)

The Star Online is an asset of Triangle Consulting Social Enterprise Ltd (hereby known as “our” or “we”.)

2. Purpose and scope

The purpose of this statement is to:

- Demonstrate how the Star Online complies with relevant legislation, including:
    - the EU General Data Protection Regulation (2016) and the UK Data Protection Act (2018),
    - the Australian Privacy Act 1988 and Australian Privacy Principles ('APPs'),
    - the common law duty of confidentiality and all other relevant national legislation.
- Document our recognition of data protection as a fundamental right and our commitment to embracing the principles of data protection by design and by default.
- Demonstrate how our data security policy is in line with the requirements of the NHS Data Security & Protection Toolkit (DSPT) in the UK
- Document how we have implemented appropriate organisational and technical measures to uphold this policy.

The scope of this policy is:

- The Star Online web application – www.staronline.org.uk
- Triangle Consulting Social Enterprise Ltd. management of the application, including management of sub-contractors
- All data which we process in relation to the Star Online web application, which includes special categories of data.

3. Overview of Star Online web application

The Star Online system is an online web application supporting organisations to use the Outcomes Star™ by accessing Star resources, entering Star data and service user information, analysing and reporting on this data.

The Outcomes Star™ is a tool used under licence by services of various sectors, such as the health and social care sectors, to assess and support the progress that service users make while they are supported by the services.

The Star Online is owned and operated by Triangle Social Enterprise Ltd (company registration number 07039452, registered address Preston Park House, South Road, Brighton, East Sussex, BN1 6SB.) Triangle are a joint data controller with organisations who purchase accounts for the Star Online.

Triangle sub-contract development and maintenance of the Star Online to Quality Education Solutions Ltd (company registration number 04700102, registered address Unit 3, Damery Works, Damery Lane, Woodford, Berkeley, GL13 9JR.)

QES sub-contract the hosting of the Star Online servers to Microsoft Azure.

QES and Microsoft Azure are data processors.

4. Underpinning policies & procedures

This policy is underpinned by the following:

- Triangle's Risk Register – assesses all risks facing the organisation including to data security, information governance and 'clinical risk' (to service users) of the Star Online;
- Annual Statement of Internal Control in regard to information risk
- Star Online Data Protection Impact Assessment (DPIA) - assesses our data processing responsibilities and risks in line with guidance from the UK Information Commissioners Office;
- Star Online Information Asset Register (IAR) and Record of Processing Activities (ROPA) – details the ways the Star Online stores and uses data, including the retention timetable;
- Star Online Helpdesk Data Security Procedure and Account Closure Procedure – sets out the rules and steps Triangle staff providing the Helpdesk service for the Star Online follow to comply with this statement;
- Star Online Emergency Incident Response Procedure – outlines the steps and communication required in any emergency incident relating to the Star Online including the reporting of any data security breach;
- Star Online Change Management Procedure – outlines the approaches taken by Triangle and our sub-contractors for the Star Online to ensure changes to the application are in line with this Information Governance Statement;
- Star Online Disaster Recovery Procedure - outlines the procedures in the event of a security failure or disaster affecting digital systems including the Star Online and those necessary to the day to day running of our organisation;
- Star Online Governance Framework – outlines the lines of responsibility for managing the Star Online and the adherence to this Data Protection Policy;
- Star Online Data Security Programme – a programme of training for Triangle staff with privileged user roles for the Star Online;
- Star Online Role Based Access Model and Personnel List – documentation of Triangle and sub-contractor staff with privileged user roles;
- Star Online Anonymisation Policy – documentation of our approach to effective anonymisation and depersonalisation of personal and sensitive data;
- Triangle Data Protection Policy - provides staff generally across Triangle with clear guidance on the collection, handling and disclosure of data collected whilst supporting organisations.

5. Star Online and personal data

5.1 The data stored on the Star Online

A full list of data stored on the Star Online database is set out in Appendix 1.

The data subjects that the Star Online holds information on are:

a) an employee of the organisation with a Star Online account and who undertakes the role of the Account Lead;

b) employees of the organisation with a Star Online account and who are assigned a licence and login to the account by the Account Lead;

c) individual citizens that use services from the organisation with a Star Online account, such as those provided in social care and health settings typically run by local authorities, charities, government or businesses.

Triangle does not have a direct relationship with the data subjects who are individual citizens, and these data subjects are not provided with direct access to our system.

Triangle holds legal agreements with the organisations with a Star Online account governing their use of our outcomes tools and our system and providing us with the lawful basis on which to process their data in the Star Online. By accepting the terms of the agreement, organisations agree to the storing and processing of data by Triangle, confirm their role and responsibility as a data controller and confirm their responsibility for protecting the personal information of the data subjects that they enter into the Star Online system, including the collection of that data on an appropriate lawful basis.

5.2 Our approach to personal data

We acknowledge our accountability in ensuring that personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- Accurate and kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’);
- Processed in a manner that ensures appropriate security of the personal data.

In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

5.3 Lawful basis for data processing

The lawful basis for processing data belonging to employees of an organisation with a Star Online account is contract, and separate consent is therefore not required.

The lawful basis for service user data is legitimate interest as we process service user data to fulfil our contractual obligations to an organisation with a Star Online account and do not have a direct relationship with service users.

The organisation purchasing the Star Online account is responsible for identifying an appropriate lawful basis on which data is collected and stored in the Star Online.

5.4 Upholding personal data rights outlined in the GDPR

- We uphold the personal data rights outlined in the GDPR:
    - The right to be informed;
    - The right of access;
    - The right to rectification;
    - The right to erasure;
    - The right to restrict processing;
    - The right to data portability;
    - The right to object;
    - Rights in relation to automated decision making and profiling.

As Triangle do not have a direct relationship with the data subjects who are individual citizens, we enact these rights through providing services to and working with the Account Lead, following our detailed Helpdesk Data Security Procedures documentation.

5.5 Data retention

Whilst a Star Online account is active, the data within it is retained unless the organisation or users remove or change it using the auditable data change features available with the Star Online. Where users cannot directly delete or change data from the user interface of the Star Online, there are procedures to enable the organisation to request this of the Star Online Helpdesk service provided by Triangle.

When a Star Online account is closed, Triangle will automatically fully and effectively anonymise all data in the account 3 months after the agreed closure date in accordance with our Anonymisation Policy. The data will then no longer be classed as personal data and will be stored by Triangle indefinitely to support our programme of research and learning around outcomes.

Organisations are given the opportunity to opt out of the anonymisation and for their data to be permanently and completed deleted 3 months after the agreed closure date.

6. Star Online responsibilities and governance

The Star Online is overseen by Triangle's Company Board in accordance with our Governance Framework, which involves monthly reporting, a minimum of a quarterly review and bi-annual planning and risk management.

In line with legislation, we have a Data Protection Officer (DPO) who reports to the highest management level of the organisation:

- Name: Hugh Collard, Chief Operating Officer, 8Fold Governance
- Title: External specialist DPO
- Contact: hugh@8foldgovernance.com and info@8foldgovernance.com

We also have a Senior Information Risk Owner (SIRO) who manages risks associated with the Star Online and data security and contribute to the regular review of Triangle's Risk Register:

- Name: Sarah Owen
- Job title: Product Director
- Contact: saraho@triangleconsulting.co.uk

7. Star Online sub-contractor management

Triangle sub-contract the capability to maintain, develop and host the Star Online so that we can benefit from the expertise, scale and governance of an external specialist organisation.

Before appointing a sub-contractor, Triangle will always undertake thorough due diligence when appointing a sub-contractor including accreditation to industry standards, references and testimonials. We will also conduct thorough tendering processes to ensure that sub-contractors demonstrate relevant experience and expertise. Triangle will also ensure that these processes apply to any sub-contracting that Triangle allow our sub-contractors to undertake (see below.)

Triangle will always include specific requirements in a sub-contractor contract covering:

- Location of data and the servers and hosting of data to be held within the UK
- Compliance with GDPR and any other relevant data legislation
- Software design and management best practice including well-supported, up to date platforms and frameworks, and accreditation with relevant certification bodies
- Cyber security best practice including adherence to the UK's National Cyber Security Centre's 14 Cloud Principles and management of OWASP vulnerabilities
- A thorough procedure for identifying, reporting, responding and addressing any data or information security incidents
- Restrictions around sub-contracting, either completely or at least without prior approval of Triangle
- Performance and uptime expectations, including a guaranteed 99% uptime.

Triangle will closely manage all contracts including at least an annual contract delivery review with the Company Board as part of our Governance Framework for the Star Online.

8. Star Online accreditation

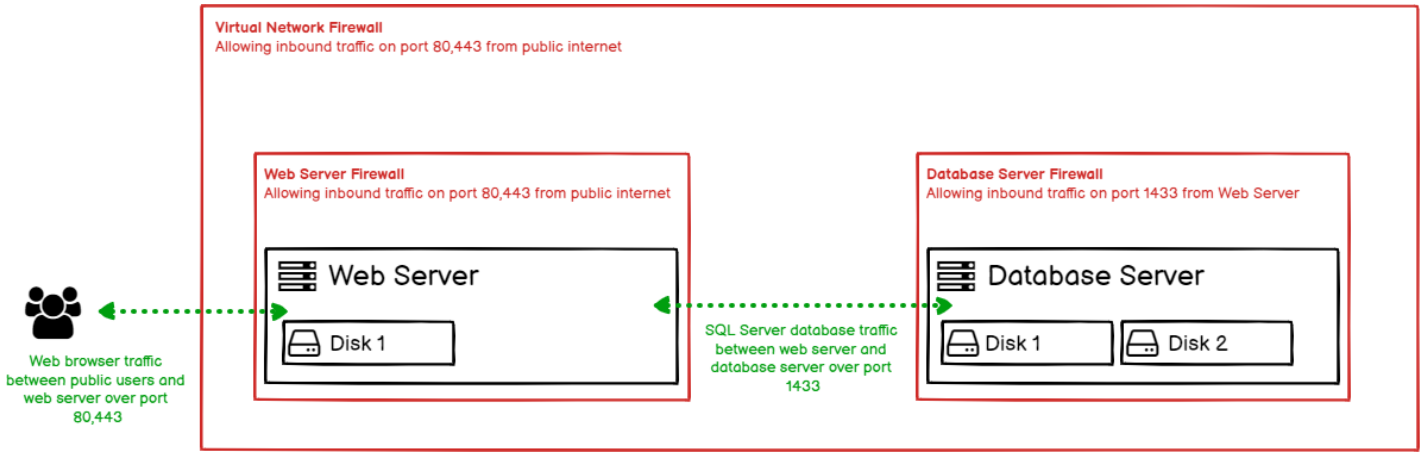
Triangle have Cyber Essentials certification.

QES have the following certification:

- ISO27001 – certificate number: 14123656
- ISO9001 – certificate number: 14131696
- Cyber Essentials Plus
- As an organisation they have N3/HSCN connections to the NHS pipeline (please note this is not currently used in conjunction with Star Online).

9. Star Online security architecture and controls

This section sets out the technical set up of the application and how that delivers data security. We aim to comply with the UK National Cyber Security Centre's Cloud Principles (https://www.ncsc.gov.uk/collection/cloud-security.) This technical security diagram shows an overview of the approach in place:



9.1 Data in transit and at rest protection

All transportation of data between application and database is done over a TLS1.2 encrypted channel. The Star Online will not support TLS1.0 from March 2022.

Our application uses PBKDF2 and SHA256 encryption and benefits from server-side encryption using Service-Managed keys through Microsoft Azure.

9.2 Physical location and legal jurisdiction

The Star Online is hosted on Microsoft Azure servers. Azure primary datacentre is in South West, UK. Azure secondary paired datacentre is in South, UK, giving us full Geo-Redundant Storage.

The server configuration is mirrored between two hypervisors, with automatic failover between the two in event of hardware failure. All data is stored on a fully redundant Storage Area Network.

9.3 Data centre security

Access to Microsoft Azure servers is limited by location and only approved individuals. Microsoft Azure provide us with a private cloud offered over a private internal network. Azure holds industry standards including CSA STAR Certification, ISO 27001, ISO 27017, ISO 27018, ISO 20000-1, ISO 9001, HIPAA, FedRAMP, SOC 1, SOC 2, UK G-Cloud.

9.4 Data sanitisation

All data from Star Online accounts is held in the cloud and no data is stored on Triangle or QES devices. All devices used by Triangle and QES are securely sanitised at the end of their life using a Secure Erase Wipe Method or similar.

Whilst a Star Online account is active, the data within it is retained unless the organisation or users remove or change it using the auditable data change features available with the Star Online. Where users cannot directly delete or change data from the user interface of the Star Online, there are procedures to enable the organisation to request this of the Star Online Helpdesk service provided by Triangle.

When a Star Online account is closed, Triangle will automatically fully and effectively anonymise all data in the account 3 months after the agreed closure date in accordance with our Anonymisation Policy. The data will then no longer be classed as personal data and will be stored by Triangle indefinitely to support our programme of research and learning around outcomes.

Organisations are given the opportunity to opt out of the anonymisation and for their data to be permanently and completed deleted 3 months after the agreed closure date.

9.5 Resilience and availability

Triangle guarantee an uptime of not less than 99.9%.

We guarantee a transfer time/speed target of less than 4 seconds on average for end users of the Software located in the UK, and aim for a transfer time/speed target of less than 4 seconds of average for end users of the Software located outside of the UK.

We ensure that scheduled downtime is managed at minimal disruption to users and outside of working hours as much as possible.

We actively monitor system uptime, server resource use and performance using automated monitoring alerts and respond to any alerts using our Incident Response Procedure (see section 1 for more detail.)

The Star Online has a Disaster Recovery Procedure (DRP) in place for and the process of restoring code from the code repository and data from the backup is regularly used.

Recovery point objective

The database runs under a backup policy that ensures in the event of a complete system failure, the maximum amount of data loss that could occur is 5 MB or 30 minutes.

Full backups are taken daily, and differentials are taken every 30 minutes or increment of 5mb (whichever comes first). Backups are Geographically Redundant of the datacentre delivering 99.9999999999999999% (16x9s) availability.

Recovery time objective

The contracted RTO to Triangle is 24 hours. The server has been configured with the Azure Site Recovery feature, meaning we have an idle secondary server in a separate datacentre that we can recover service to within 15 minutes. (The last test of this took 8 minutes).

In the case of a full data centre failure, the service would be reinstated to within 5 minutes of when the event occurred. Return to service time will be <1 hour.

9.6 Data separation

QES store all data for each system they maintain in distinct, separated databases, with unique SQL logins. There is no possibility of any data being shared from other systems as a result of this architectural approach.

On the Star Online, all data is restricted to each individual account. QES and Triangle take data security seriously with any staff able to access data in an account trained in data security procedures.

9.7 Secure development and change management

Change to the system is managed as per our Change Management procedure, and we adhere to security by design principles.

The application is periodically tested for vulnerabilities by a permanent member of the development team who has been trained in CREST Ethical Hacking and penetration testing. QES development team run monthly “Hackathons” whereby they attempt to hack into our application in a test environment which mimics that of the production environment. The findings of this are then fed into the development sprints for remediation.

The software is also continually tested using our automated testing model through TFS Build and Release. Through continuous integration (DevOps and DevSec) we are able to use established tools which specialise in checking for vulnerabilities but also build our own custom tools which run every time we make a change to the system.

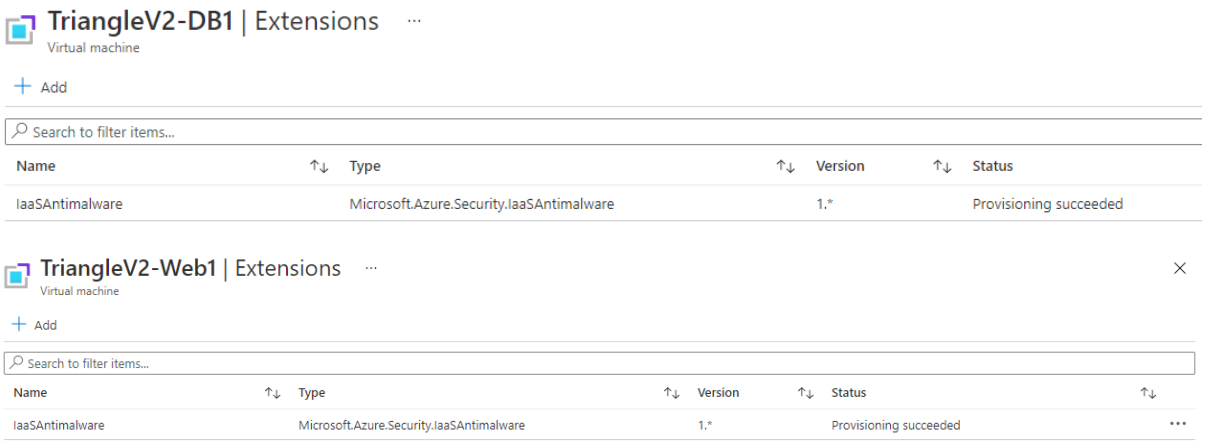
An example of a few we have integrated:

- SonarQube - a code quality tool which checks for bugs and vulnerabilities in the code in line with OWASP. (https://www.sonarqube.org/)
- OWASP ZAP (Zed Attack Proxy) – Vulnerability scanner (https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)
- Custom built – API anonymous scanning – Ensures that there are no vulnerable APIs
- Custom built – Web.config checks – Ensures all security keys are enabled.

9.8 Vulnerability management and intrusion prevention

A penetration test is completed on the application annually by an external specialist. The most recent pen test was completed in February 2023 by the NCC Group. A summary of results is available separately on request.

The system uses Microsoft Defender Antimalware managed through Microsoft Azure.

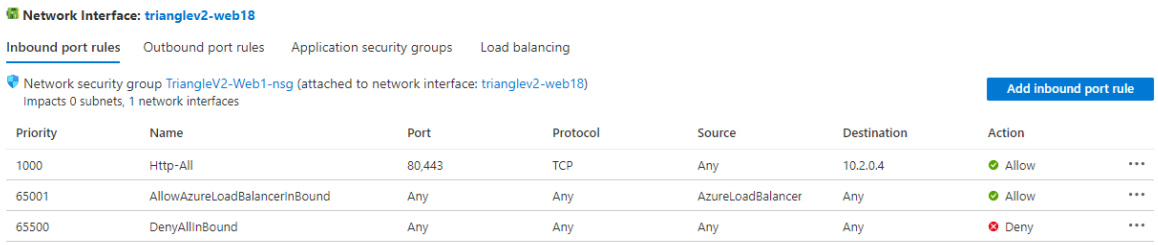


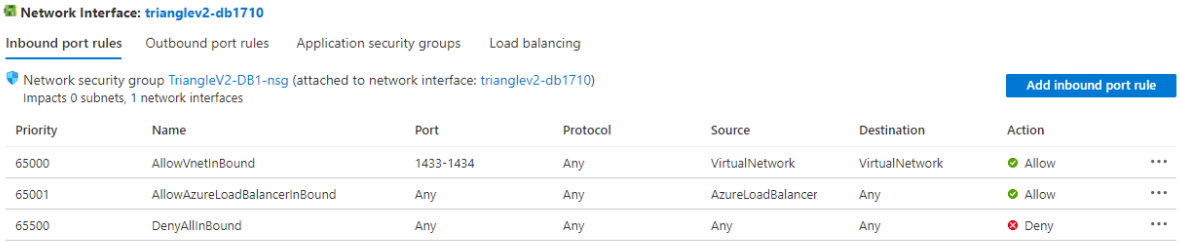
We have a dynamic approach for patch management:

- Critical, low risk updates to the server automatically take place the day they are issued by Microsoft. All other updates are tested on our STS and UAT environment prior to release.
- Application patches are tested in the same environments prior to a production release.
- OS Host updates are managed using Azure Update Management and scheduled during agreed maintenance windows with Triangle.

Firewalls are managed through Microsoft Azure. All open ports and services have been subject to justification and approval by an appropriately qualified and authorised business representative, and this approval has been properly documented.

There are policies in place to ensure that all firewall rules that are no longer required are to be removed or disabled in a timely manner, and there are currently no open ports or services that are not essential for the business.





The remote administrative interface has been disabled on all firewall devices. Only web traffic is enabled on the Triangle Application Server. Only SQL Server ports are enabled from inside the virtual network on the database server.

9.9 Protective monitoring

Our servers have built in Denial of Service attack (DDoS) protection. Azure monitor and inform us of any suspicious activity (intrusion detection) on the server and we have built custom proactive monitoring alerts that will notify of immediate or impending service failure, or suspicious activity to be investigated.

Triangle are signed up the NCSC Early Warning System for the Star Online domains and IP addresses.

9.10 Personnel security

See Appendix 1 for a description of the Role Based Access Model in use. A full breakdown of current personnel and their access to privileged user roles for the application is available on request as this breakdown is continually monitored and updated. Star Online Manager/SIRO manages access to privileged security roles as part of Triangle's JML (joiners, movers, leavers) policy.

As part of QES's readiness programme, QES has specifically upskilled staff in two areas; GDPR readiness and CREST Technical Application Security testing, enabling us to better understand and implement defensive measures against threats to data security and integrity. All staff have been trained and made aware of GDPR and the ICOs Think.Check.Share guidance. All QES staff are DBS checked.

Triangle staff with access to data within Star Online accounts via privileged user roles is limited to the helpdesk. Helpdesk staff undertake regular training in data protection and security as part of the Star Online Data Security Programme using modules built from from the ICO and National Cyber Security Centre guidance.

9.11 Device security

All devices at QES are protected with Microsoft Defender Antimalware and company policies such as encryption, email filters, web traffic control, and portable device ports locked down.

Triangle devices are protected in line with the following illustration from our IT security provider, It's What's Next (Milton Keynes) CIC.

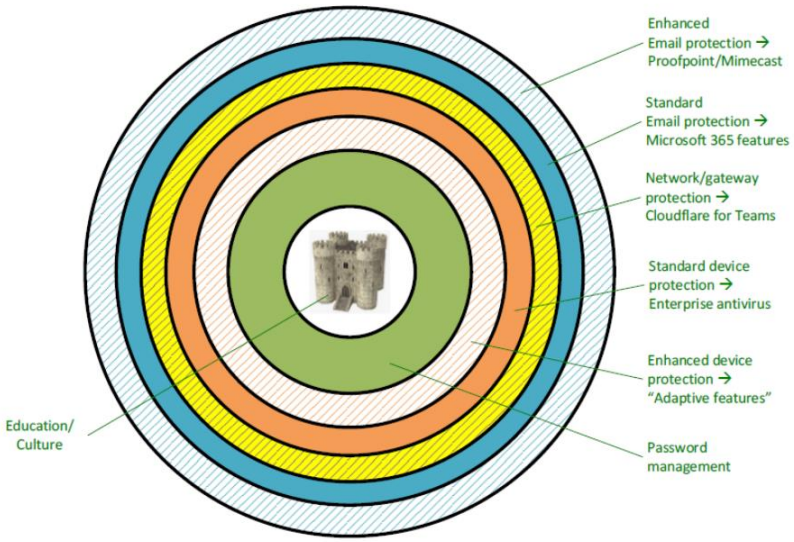


Figure 1: IWN-IT Layered Cyber Security Framework illustration

In addition to the security settings applied above, acceptable use policies ensure that staff use good practice including preventing the use of public WIFI or personal devices for all QES and Triangle's Star Online Team personnel for accessing the application via a privileged user role.

9.12 End user identity and authentication

Multifactor authentication for all users

Two Factor Authentication is enabled. In addition to the username and password, users are sent a one-time access code by email when they login every 24 hours and per unique IP address. This must also be entered before a user is authenticated with the system.

Strong passwords

Star Online requires strong passwords (minimum 10 characters, including upper case, numerical and special character) and enforces a new password every 3 months. In addition, users cannot use previously used passwords and user account lockout occurs after 10 failed attempts.

User Accounts are managed directly by organisations within their accounts.

All user accounts require 2 factor authentication every 24 hours.

9.13 Secure service administration

We utilise a dedicated devices for service administration approach in line with UK National Cyber Security Center guidance, with a dedicated machine for service management that QES use to access the host devices that run the Star Online application. This machine has restrictions in place to limit the use to only service management actions and has the same security settings that apply to the Star Online and other applications that QES manage that are also used by public sector organisations and so require the same security architecture and permissions.

10. Audit information

All server administration actions are audited in Azure and a full application audit history stored in the system database.

Full audit logs for all activity in an account are available on request from the Star Online Helpdesk. Account Lead to email the Helpdesk and make a request for the audit log or specific activity within the audit log for your account. Data will be shared via a secure file sharing service specified by the client organisation or made available within the interface of the Star Online account.

Currently, only the development team at QES and those with Super User access at Triangle are able to view the audit log. The data in the audit log cannot be amended. Audit logs are retained for as long as the account is active.

See Appendix 3 for more information.

11. Star Online incident reporting and management

In the case of an emergency incident, Triangle's Emergency Response Procedure would be followed. Full information is available as a separate document, but in summary this procedure involves:

- Alerting the primary emergency incident contacts at Triangle and QES immediately - QES will acknowledge any notifications of business-critical incidents within 1 hour.
- Ongoing communication with clients affected by the incident through the Helpdesk.
- Work within the decision framework set out in the Disaster Recovery Plan.
- QES will aim to resolve the service being unavailable within 1 working day, or within 5 days for other business critical issues.
- All fixes and resolutions including restoring the system will be discussed with Triangle, thoroughly quality assured and tested by QES' testing team and tools and signed off by Triangle before implementation.
- Documentation of the issue in Incident Report including thorough investigation into the incident, analysis of action taken, sequence of events, learnings taken forward.
- Review and discussion of Incident Report at Company Board level including the communication to relevant authorities (such as reporting to the UK Information Commissioner's Office) and to the data subjects affected.

12. Review

This document will be reviewed and updated by 1st July 2024 at the latest.

Appendix 1: Star Online and Role based access control (RBAC)

Security role	Permissions and access
Azure Network Administrator	• Manage security settings including firewall, incident monitoring and patch updates
System Administrator	• Create, Read, Update, Delete (CRUD) in SQL databases for Live and development environments • CRUD codebase of application – Live and development environments - in Azure Dev Ops • Push releases
Quality Assurance	• Read only in SQL databases for Live environment • CRUD for SQL databases and codebase in Development environments
Super User	• CRUD Star frameworks, lists, post-login pop up and broadcast notifications • CRUD Help Centre content
Super User – Training environment	• CRUD Scenarios in Training site
Helpdesk	• CRU Accounts • Edit licences available to Accounts • CRUD Users • CRU data in all Accounts and Delete for specific data including actioning service, engagement, user deletion requests
Account Lead (Client role)	Within authorised Account: • Accept Star frameworks • Create and edit Services • Create and edit Users including deactivating users • View and edit all data including actioning Star and service user deletion requests
Service Manager (Client role per service)	Within authorised Service: • Create and edit Users • View and edit all service user data including actioning Star and service user deletion requests • View Star resources
Practitioner (Client role)	Within authorised Services: • View and edit service user data • View Star resources
Licensed Trainer (may also be Account Lead, Service Manager/Practitioner)	• View Star Training resources in Live environment • Access Training environment and set up training sessions using existing scenarios

Appendix 2: Data stored on the Star Online

All users of the Star Online must provide a valid email address, password, first name and last name in order to log in and gain access to the application and resources it contains.

Organisation name, type and location is also recorded and we collect some activity in order to support use of the system, e.g. the date and time of the last login.

In addition to the information we hold on all active Star Online users, we hold the service names, service types, locations of users. We also record their activity within the system, for instance, the last time they logged in, and if, when and for which client they've entered Star readings and action plans or requested Star readings be deleted.

Information the Star Online system will process on service users is set out below.

Service user information

Service user records are created and managed by organisations using the Star Online, there is no 'service user' user account type and so we don't require or use an email address or password for service users.

Personal data relating to service users can be stored securely within the system, including:

- First name and Surname and/or Unique ID reference
- Preferred name (optional)
- Service names and Star versions being used with that individual
- Start and end dates of support (engagements)
- Star readings, completion information and Notes – see below for more information
- Action Plans and Other Notes (optional) – see below for more information

The following information can be added to the service user record:

- Address (optional)
- E-mail address (optional)
- Phone (optional)
- Gender (optional)
- Ethnicity (optional)
- Support needs (checkboxes are provided relating to the likely support needs depending on the Star used with a service user)

All of these fields are optional, so they can be left blank. If the same information is stored in another system or the Star Online isn't used for reporting it may not be necessary to also capture the information on the Star Online service user record and organisations.

Star readings

Organisations can enter multiple Star readings for service users. For each Star reading, there are a number of areas covering the different aspects of a person's life. For each area there are a series of

numbered statements describing where the service user might be – text descriptions of the person's current situation, behaviour and attitudes – from which the worker and service user collaborate to make a choice. Notes can be entered in free text fields for each area to enable workers to expand on the "reading" selected.

Action plans

The Star Online action plan feature is optional. It enables workers to record notes in a free text field about one or many areas of the Star and automatically includes the "reading" number selected for each area included in the action plan.

Other Notes

This feature allows other related data to be stored against a service user's record and engagement, such as number of other individuals in their household or school attendance figures. Currently this feature is being piloted and only available to a small number of organisations. Access to each Other Notes type is controlled by the Helpdesk and all are disabled as default.

Appendix 3: Audit log and list of events

User log in success	Service viewed
User updated	Service created
User created	Service updated
User password reset	Service deleted
View user	Service deactivated/archived
Lookup value updated	Star type distributed
User log in failed	Service user viewed
User password updated	Service user created
Account viewed	Service user updated
Account created	Service user deleted
Account updated	Engagement created
Account Frozen	Engagement ended
Account Blocked	Engagement updated
Account deleted	Star entry created
Audit details viewed	Star entry updated
Audit list viewed	User profile updated
Star type viewed	User profile viewed
Star type created	User licence deactivated
Star type updated	User licence reactivated
Star type deleted	User deleted
Account activated	Data request created
	Data request viewed
	Data request completed
	Data request cancelled
	Data request rejected
	Data request approved
	User session error

Appendix 4: Age Appropriate Design UK Code

1. Introduction and applicability to the Outcomes Star Online

Developed by the Information Commissioners Office in the UK, this code explains how to ensure online services appropriately safeguard children's personal data and came into force in the UK on 2 September 2020.

(For organisations in Australia, please note that the 'UK Code' is likely to be the basis of changes to the Australian Privacy Act planned for 2024 following the 2023 review.)

Triangle have defined that Outcomes Stars and Outcomes Star Online (OS) are covered by the code as they process personal data, they are likely to be accessed by children (in relation to specific versions such as My Star, Shooting Star, My Mind Star, Attention Star, Youth Star) and they are an 'information society service.'

Importantly Stars are different to most services covered by the code, because the primary audience for OS are the practitioners who use the Stars with children, young people and adults, rather than directly to the children, young people and adults themselves. Children and young people do not have logins to OS, it would not be accessed from the device of a child or young person, and the child or young person cannot access it without the direction and 'control' of the practitioner using the Star.

It is therefore the responsibility of the practitioner and the service choosing to use the Star with the child or young person to do so in a way that is compliant with legislation and best practice. However, as they are still accessible by children, we have used the code to guide our design designs and demonstrate our compliance here.

2. Compliance to the 15 Standards

1. Best interest of the child

Aligned with Article 3 of the United Nations Convention on the Rights of the Child (UNCRC), we have considered how OS use of data impacts on children's rights and needs and accounted for the best interests of the child as a primary consideration.

In our use of personal data belonging to children and young people, we have considered how we:

- keep them safe from exploitation risks, including the risks of commercial or sexual exploitation and sexual abuse;
- protect and support their health and wellbeing;
- protect and support their physical, psychological and emotional development;
- protect and support their need to develop their own views and identity;
- protect and support their right to freedom of association and play;

- support the needs of children with disabilities in line with your obligations under the relevant equality legislation for England, Scotland, Wales and Northern Ireland;
- recognise the role of parents in protecting and promoting the best interests of the child and support them in this task; and
- recognise the evolving capacity of the child to form their own view, and give due weight to that view.

Stars for children and young people are designed through participatory research with children, young people and with services who are experts in supporting children, to ensure that all content is safe and appropriate.

We make privacy information and consent forms available in an accessible easy-to-read format.

Children who can form their own views have rights to express them, in all matters that affect them. Stars support children to have a voice and to encourage services to listen to children holistically.

Completed Stars and Star completion is designed to be private between practitioner and child/young person. There is no 'community' platform within OS or functionality for data belonging to one data subject to be directly shared with another data subject. There are safeguards built into OS to prevent human error in data being shared with unauthorised users.

The data collected is controlled by the practitioner and the service they work for (the client organisation) and it is private to that service.

Triangle have strictly limited processing of this data and do not share it with any third parties apart from those named as sub-processors for the purposes of fulfilling our contract with the client organisation. This includes not using any contact details recorded for any service user on the OS (child, young person or adult) for any purposes whatsoever, including contacting the child directly for any purposes.

Triangle have a dedicated Clinical Safety Officer who regularly assesses the product and service for clinical safety risks and supports with the minimisation and mitigation against risks.

2. Data Protection Impact Assessments

We regularly complete DPIAs.

In January 2024 we are auditing all our DPIA and data protection documentation and onboarding an external, specialist Data Protection Officer.

We will publish an updated DPIA by March 2024.

3. Age Appropriate Application

We aim to apply the standard to all service users whose data is stored within OS whether they are children or not.

We do not use any age assessment technology. Where age is recorded, this is at the discretion of the service and practitioner and it is used for informational purposes for the service and practitioner only, it does not affect the functionality or performance of OS in any way.

4. Transparency

We provide service user consent in accessible format.

We are introducing bite-size prompts throughout our new live completion screens including options to go to more detailed information as needed. This will be available in April 2024, which will provide guidance using the 'just in time notice' approach.

5. Detrimental use of data

OS is not impacted by any of the areas highlighted by the ICO under this principle, such as marketing, gamification, or rewards.

Triangle do not contact data subjects directly and are strictly limited as to how their personal data can be used under our contract with client organisations.

6. Policies and community standards

Triangle uphold our Privacy Notice standards and adhere to our Information Governance Statement and all other policies and legislation relevant to OS.

We regularly audit and assess ourselves against our policies, including through external assessment with our outsourced Data Protection Officer and Clinical Safety Officer.

7. Default settings

OS defaults relating to privacy are controlled by the practitioner or service providing the service to the child or young person, rather than the data subject themselves. As there are strict limitations to how personal data of data subjects can be used, there isn't a significant difference between the default settings relating to privacy and the settings that be configured.

Data subject's data is always restricted to access only by authorised users (authorised by the service) and is always treated as sensitive personal data, even when fields such as name and data of birth have been disabled.

8. Data minimisation

We follow the principle of data minimisation for all data subjects, including children and young people, and for all users, including those who support children and young people. OS does not seek to extract more data than the minimum that is required for effective use of the tool – there is no value to OS or Triangle in extracting more data.

As OS is not customisable – eg users cannot add their own fields or forms – there is robust control and classification of the data being stored about data subjects, including the completion of DPIA where there are any significant changes or expansion to the data being stored.

9. Data sharing

The data collected is controlled by the practitioner and the service they work for (the client organisation). Triangle have strictly limited processing of this data and do not share it with any third parties apart from those named as sub-processors for the purposes of fulfilling our contract with the client organisation.

10. Geolocation

OS is not used on the device of a child or young person. It is used on the device of the practitioner providing support to the child or young person.

Regardless geolocation technology is not used within OS. The IP address of a user is recorded but this information is not made available within OS, it is recorded within private audit logs that are only available to authorised administration-level users on request.

11. Parental controls

OS does not provide any parental controls because it is not being accessed directly by a child or young person, it is being used under the supervision and direction of a practitioner.

12. Profiling

We do not use any AI or algorithmic or machine learning. We do not do any profiling.

13. Nudge techniques

OS does not use any nudge techniques to drive a data subject into any specific behaviour. OS does not seek to extract more data than the minimum that is required for effective use of the tool – there is no value to OS or Triangle in extracting more data.

14. Connected toys and devices

Not applicable for OS.

15. Online tools

As use of the OS will always be under the direction of a practitioner, action buttons such as ‘Help’ are geared towards them rather than directly to data subjects.

Our Privacy Notice and consent documentation provides clear information on how data subjects can enact their rights relating to their personal data.

3. Accountability and review

This policy and our adherence to the code is the responsibility of our Senior Information Risk Officer who is a member of the Company Board.

It will be reviewed and updated in line with our Information Govnernance Statement, at least annually.

The next review will take place by July 2024.